Department of Homeland Security Daily Open Source Infrastructure Report for 16 December 2005

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports a storm with freezing rain and ice across Georgia and the Carolinas early Thursday, December 15, closed schools, snarled traffic, and caused power outages to more than 350,000 customers. (See item 3)

- The San Francisco Chronicle reports whooping cough, a disease that was largely tamed by vaccination, has been making a comeback throughout California, killing seven so far this year while the number of reported cases throughout the state has doubled. (See item 25)

- KLASTV reports Las Vegas police are using a program known as "City Watch" that connects the city to every security system on the Las Vegas Strip, to help prevent terrorist attacks and respond to disasters. (See item 28)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *December 15, MarketWatch* — **FERC approves Duke−Cinergy merger.** The deal struck between Charlotte, NC−−based Duke and Cincinnati, Ohio−based Cinergy was announced in May after the two agreed to a $9.1 billion stock swap. The combined company would have assets of about $70 billion and serve about five million electric customers. The commission said

that transaction it approved would create a company with 45,000 megawatts of electric generating capacity and 17,500 miles of natural gas pipelines, with customers in Kentucky, Indiana, North Carolina, Ohio, South Carolina, and Canada. Federal Energy Regulatory Commission (FERC) approval of the deal had been widely expected by industry analysts. The deal still needs final approval from state utility regulators in Ohio, North Carolina, and Indiana as well as the federal Nuclear Regulatory Commission, Federal Communications Commission, and the shareholders of both companies. Duke and Cinergy said they still expect to have gathered all the necessary approvals to complete the deal in the first half of 2006.
Source: http://www.marketwatch.com/news/story.asp?guid={A5243B4F−5E00−4DDF−BFF8−3ACBAF24496C}&siteid=google

2. *December 15, Government Accountability Office* — **GAO−06−275: Natural Gas and Electricity Markets: Federal Government Actions to Improve Private Price Indices and Stakeholder Reaction (Report).** Since the 1970s, the natural gas and electricity industries have each undergone a shift toward greater competition, referred to as restructuring. This restructuring has moved these industries from regulated monopolies to markets in which competitors vie for market share and wholesale prices are largely determined by supply and demand. Amid this restructuring, private companies have published information about these markets, including reports of market prices in various locations −− referred to as price indices. Market participants rely on these price indices to help them make informed decisions about trading these commodities and to evaluate new investments. In this context, the Government Accountability Office (GAO) agreed to answer the following questions: (1) What federal regulatory and statutory efforts have been taken to improve price indices in electricity and natural gas markets? (2) Have federal efforts improved industry stakeholders' confidence in these price indices? Stakeholders told GAO that, because natural gas is widely used to generate electricity, their prices often move together and, therefore, natural gas forward prices can substitute, to some extent, for electricity futures prices. They also said that the use of these natural gas markets only partly mitigates the lack of robust long−term electricity markets, because electricity and natural gas prices sometime move independently.
Highlights: http://www.gao.gov/highlights/d06275high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−275

3. *December 15, Associated Press* — **Icy storm cuts power to 350,000 in South.** A jolt of freezing rain and ice across Georgia and the Carolinas early Thursday, December 15, closed schools, snarled traffic, and caused power outages to more than 350,000 customers. The outages were caused by ice that formed on tree limbs and fell onto power lines. About 160,000 were without power in South Carolina's upstate, 102,000 in northeast Georgia, 57,000 in the Atlanta area, and 40,000 in western and central North Carolina. School systems canceled or cut short classes from northern Georgia to western stretches of Virginia. The National Weather Service said the freezing rain was expected to continue in the region through Thursday evening and overnight temperatures were forecast to dip into the 20s. More power lines and tree limbs could snap under ice layers expected to grow to up to three−quarters of an inch thick. Mountains of North Carolina and Virginia were being hit with a hazardous mix of snow and sleet, with accumulations from one to three inches expected overnight. A spokesperson for Duke Power, the main supplier of electricity in the hard−hit stretches of the Carolinas, said crews were working to restore power, but added that it could be a long process.
Source: http://www.chicagotribune.com/news/nationworld/sns−ap−ice−st

orm,1,4593623.story?coll=chi−news−hed

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *December 14, Journal News (NY)* — **Barge spills diesel fuel into Hudson River.** A K−Sea transportation barge spilled about 6,500 gallons of diesel fuel into the Hudson River last week, the Coast Guard said Tuesday, December 13. The KTC−55 barge leaked low−sulfur diesel fuel as it was being pushed upriver Thursday, December 8, by the tug Baltic Sea on a daylong trip from Staten Island to an Exxon Mobil terminal at Albany, NY, Coast Guard spokesperson Dan Bender said. A small crack or hole that has yet to be identified is believed to be the cause of the trickling leak, Bender said. Shortly after the barge arrived in Albany at about 9:30 p.m. EST, the crew noticed "diesel oil bubbling up along the side of the barge on the port side," Bender said. Crewmembers then reported the spill to a national hotline, and a test showed one of the barge's chambers had lost about 6,500 gallons in transit, Bender said. Environmental damage from the spill should be "minimal," Bender said, because the fuel trickled out over the course of a day and more than 140 miles.
   Source: http://www.thejournalnews.com/apps/pbcs.dll/article?AID=/20051214/NEWS05/512140303/1025/NEWS09

5. *December 13, WNCT−TV 9 (NC)* — **Gasoline spill in North Carolina county prompts highway closure.** A truck overturned spilling more than 2,000 gallons of fuel on North Carolina Highway 17 on Monday, December 12, just north of Calabash in Brunswick County, NC. A portion of the highway was closed for more than seven hours. The tanker truck leaked more than 1,500 gallons of gas and 900 gallons of diesel fuel. No one was injured. The remaining fuel was loaded onto another truck.
   Source: http://www.wnct.com/servlet/Satellite?pagename=WNCT%2FMGArticle%2FNCT_BasicArticle&c=MGArticle&cid=1128768694086&path=!n ews!localnews

[Return to top]

Defense Industrial Base Sector

6. *December 15, Government Accountability Office* — **GAO−06−171: DoD Systems Modernization: Uncertain Joint Use and Marginal Expected Value of Military Asset Deployment System Warrant Reassessment of Planned Investment (Report).** Because of the importance of the Department of Defense’s (DoD) adherence to disciplined information technology acquisition processes in successfully modernizing its business systems, the Government Accountability Office (GAO) was asked to determine whether the Transportation Coordinators’ Automated Information for Movements System II (TC−AIMS II) program is being managed according to important aspects of DoD’s acquisition policies and guidance, as well as other relevant acquisition management best practices. TC−AIMS II was initiated in 1995 as a joint services system to help manage force and equipment movements within the United States and abroad. The U.S. Department of the Army has the lead responsibility for managing the system’s acquisition and estimates its life−cycle cost to be $1.7 billion over 25

years. GAO is making recommendations to the Secretary of Defense to, among other things, develop the analytical basis needed to determine if continued investment in TC−AIMS II, as planned, represents prudent use of limited defense resources. In written comments on a draft of this report, DoD concurred or partially concurred with GAO's recommendations. It also described planned actions that are largely consistent with GAO's recommendations.
Highlights: http://www.gao.gov/highlights/d06171high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−171

7. *December 15, Government Accountability Office* — **GAO−06−66: Defense Acquisitions: DoD Has Paid Billions in Award and Incentive Fees Regardless of Acquisition Outcomes (Report).** Collectively, the Department of Defense (DoD) gives its contractors the opportunity to earn billions of dollars through monetary incentives—known as award fees and incentive fees. These fees are intended to motivate excellent contractor performance in areas deemed critical to an acquisition program's success, with award fees being appropriate when contracting and program officials cannot devise objective incentive fee targets related to cost, technical performance, or schedule. The Government Accountability Office (GAO) was asked to determine whether award and incentive fees have been used effectively as a tool for achieving DoD's desired acquisition outcomes. To do this, GAO selected a probability sample of 93 contracts from the study population of 597 DoD award− and incentive−fee contracts that were active and had at least one contract action valued at $10 million or more from fiscal year 1999 through 2003. GAO recommends that DoD improve its use of fees by specifically tying them to acquisition outcomes in all new award− and incentive−fee contracts, maximizing contractors' motivation to perform, and collecting data to evaluate the effectiveness of fees. In its comments on a draft of this report, DoD concurred or partially concurred with all of the recommendations.
Highlights: http://www.gao.gov/highlights/d0666high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−66

[Return to top]

Banking and Finance Sector

8. *December 15, SC Magazine* — **Phishers turn to blended attacks to catch more surfers.** Organized criminal gangs are targeting online consumers with ever more sophisticated blended phishing attacks −− some of which even find out details of their interests and use them to generate tailored phishing emails −− security experts have warned. As awareness has grown about phishing, the tactics used by phishers have evolved since the last holiday season. Refined phishing tactics recorded by CyberGuard include a rise in the use of automated URL obfuscation tools. With a freely downloadable tool from the Internet, the phisher simply enters the URL of the legitimate Website and then enters the address of the fake malicious website, with the tool automatically crafting a new "socially engineered" URL that includes the text from the legitimate URL. The use of embedded Java script and Active X applets is becoming more common in phishing emails. These scripts and applets can automatically place a graphic image of the expected legitimate URL on top of the address bar within the browser to hide the actual address that the browser is really being directed to. According to the Anti−Phishing Working Group, phishing is on the increase again, as the number of newly reported phishing campaigns reached 15,820 in October, an increase of 127 percent over October 2004.

Source: http://www.scmagazine.com/uk/news/article/533070/phishers−turn−blended−attacks−catch−surfers/

[Return to top]

Transportation and Border Security Sector

9. *December 15, Chicago Tribune* — **Study faults city, Southwest for Midway dangers.** Chicago and Southwest Airlines for years have "carelessly ignored" the risks of short runways and insufficient overrun areas at Midway Airport, an expert on transportation disasters said Wednesday, December 14, in a report on last week's fatal accident. The crash was avoidable, and the outcome would have been much worse if fuel tanks on the plane ruptured and caught fire, said Gunnar Kuepper, chief of operations at Emergency & Disaster Management Inc. According to Kuepper, for a fraction of the financial losses that Chicago and Southwest will pay out from the accident, the city and its major airlines at Midway should have invested in safety systems to minimize the damage of a plane skidding off a runway. The report cited similarities to a 2000 accident in which a Southwest plane overran a runway in Burbank, CA, in rainy weather and crashed into two cars on a street. Chicago airport officials say they are working with the Federal Aviation Administration on a plan to comply with a 2015 federal deadline to improve runway safety areas.
   Source: http://www.chicagotribune.com/news/local/chicago/chi−0512150275dec15,1,5609562.story

10. *December 15, American Trucking Associations* — **American Trucking Associations revises diesel fuel costs estimates for 2004 and 2005.** On Thursday, December 15, the American Trucking Associations (ATA) revised the trucking industry’s 2004 fuel costs and projected an increase in the amount it will spend on fuel in 2005. Despite recent dips in both diesel and gasoline prices, ATA said the trucking industry will spend $87.7 billion on fuel this year. This marks a $2.7 billion increase over the previous estimate of $85 billion issued in September. ATA President and CEO Bill Graves said despite recent fluctuations in energy prices, diesel costs remain the number one concern of motor carriers, representing the second−highest operating expense and accounting for as much as 25 percent of total operating costs. Higher fuel costs are hitting the trucking industry as it prepares to accept Ultra Low Sulfur Diesel fuel, scheduled to hit the market in mid−2006, and a new round of lower−emission diesel engines mandated by the Environmental Protection Agency in 2007. Each of those market changes is expected to impact the industry, driving operating costs higher.
    Source: http://www.truckline.com/NR/exeres/C622BE1A−0921−4D93−AF1F−5F42C04F07C3.htm

11. *December 15, Associated Press* — **Blown tire on landing gear causes United flight to be aborted.** A blown tire on a Boeing 737's landing gear caused the crew to abort the flight before takeoff Wednesday, December 14, at O'Hare International Airport, according to a United Airlines spokesperson. Jeff Green said no injures were reported on Flight 394, which was headed to Charlotte, NC. The plane's 95 passengers and five crewmembers were placed on buses to return to the O'Hare terminal, and a spare plane was being readied to fly the passengers to Charlotte, Green said. The plane was traveling at a very low speed when the takeoff was aborted, and stairs were brought out for use by the passengers disembarking, he said.

Source: http://www.usatoday.com/travel/news/2005−12−14−ohare−blown−t ire_x.htm

12. *December 15, KSAT (TX)* — **National Transportation Safety Board urges Union Pacific to step up safety.** The National Transportation Safety Board issued new safety recommendations Wednesday, December 14, for railroad companies, one and a half years after a deadly train derailment in south Bexar County, TX. NTSB members, who have been investigating the incident, recommended that railroads install an automatically activated device that will catch the attention of employees involved with switch operations. In addition, the board recommended that railroads place tank cars toward the rear of trains, reduce the speed of trains through populated areas, and carry breathing apparatus for crew members on trains carrying hazardous materials.
Source: http://www.ksat.com/news/5541106/detail.html

13. *December 14, Washington Post* — **New TSA surveillance tactic curtailed.** Just two days into an experimental program that would place undercover air marshals in train, bus, ferry, and other mass transit stations, the Transportation Security Administration (TSA) has scaled back its test, owing to confusion over the rollout. TSA officials had planned to deploy teams of air marshals, local law enforcement officers, and bomb−sniffing dogs at seven locations around the nation this week to test whether the agency could deter criminals in public transportation stations and conduct surveillance. On Tuesday, December 13, local officials at some of the locations said they were not participating in the program or had not been informed. TSA spokesperson Yolanda Clark said the air marshal teams, known as "Viper," for Visible Intermodal Protection and Response, would not be present in the Washington Metro system. Federal Air Marshal Service spokesperson David Adams said that Viper teams would be deployed at rail and mass transit facilities in Philadelphia, but some local officials there were not notified. The Washington State Patrol chose not to participate. Security experts expressed concern about the TSA's plans to deploy more Viper teams beyond the weeklong experiment because air marshals will be diverted from protecting aircraft.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/12/14/AR2005121402366.html?nav=rss_business

14. *December 14, Associated Press* — **Briefing: Air passenger growth to slow in 2006.** Global growth in air passenger traffic will slow next year due to a general economic slowdown, but falling oil prices could help airlines cut their losses, the industry's trade group said Wednesday, December 14. The airline industry, which will probably suffer net losses of $4.68 billion this year, could break even in 2006 if fuel prices drop sufficiently, the International Air Transport Association (IATA) said. "There is now a case for qualified optimism about the industry's financial performance," said IATA chief economist Brian Pearce. IATA expects losses next year to narrow to $4.3 billion, and forecasts the industry to a net profit in 2007. Growth in air passenger traffic for international and domestic flights is expected to drop from 7.1 percent this year to 4.5 percent in 2006, said IATA Chief Executive Giovanni Bisignani. Air passenger traffic had growth of 8.8 percent in the first six months of 2005, led by airlines from the Middle East, Latin America, and North America. The industry's overall performance, however, was being weighed down heavily by performance in the United States.
Briefing: http://www.iata.org/pressroom/speeches/2005−12−15−01.htm
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/12/14/AR2005121400432.html

[Return to top]

Postal and Shipping Sector

15. *December 15, Associated Press* — **Cargo plane runs off taxiway at North Carolina airport.** No one was injured when a FedEx cargo plane went off a taxiway and became stuck in mud at approximately 7:30 a.m. EST Thursday, December 15, at Charlotte−Douglas International Airport, authorities said. Only the crew was onboard at the time of the accident, and no injuries were reported. Despite freezing rain in the area, airport spokesperson Haley Gentry said the accident "appears to have absolutely nothing to do with the weather." Gentry said the FedEx pilot "turned short" while the plane was taxiing and became mired in mud. No commercial flights were affected by the accident.
Source: http://www.wsoctv.com/news/5541831/detail.html?rss=char&psp= news

16. *December 15, Baltimore Sun* — **Computer system missing after post office break−in.** A burglar broke into the post office in the West Friendship Shopping Center in West Friendship, MD, early Wednesday, December 14, and stole a computer system, postage printer and scanners that the postal service says have a lot of value to the government, but won't fetch much for the burglars. Without the passwords, "the computer has no use to anyone outside the post office," spokesperson Frank J. Schissler said. "Maybe they thought that they could sell the computer's guts to a pawn shop, but its guts are not a basic PC system. It was specially designed for the Postal Service." The government is offering up to a $10,000 reward for information leading to the return of the computer system, which weighs packages, calculates postage and tracks retail activity. Schissler said that identity theft is not a concern. The system tracks packages, not sender's payment information or address.
Source: http://www.baltimoresun.com/news/local/bal−burglary1215,1,6752468.story?coll=bal−local−headlines

17. *December 15, Government Accountability Office* — **GAO−06−190: U.S. Postal Service: Purchasing Changes Seem Promising, but Ombudsman Revisions and Continued Oversight Are Needed (Report).** Purchasing makes up a significant portion of annual expenses for the U.S. Postal Service (USPS). USPS has recently made significant changes to its purchasing regulations, which, according to USPS, will result in a more businesslike purchasing process. Some stakeholders, including smaller suppliers who stated they rely on USPS for the majority of their business, have raised concerns about these changes. The Government Accountability Office (GAO) was asked to (1) describe these changes, stakeholder views, and USPS's rationale for the changes and (2) assess how these changes reflect the principles of postal reform and practices of leading organizations and identify areas, if any, for continued oversight. To address inconsistencies in USPS's ombudsman, GAO is recommending that the Postmaster General revisit the intended purpose for its ombudsman, consult with experts to determine other options, and make the necessary changes in its regulations and guidance to conform with leading principles and practices. GAO provided a draft of this report to USPS for its review and comment. USPS generally agreed with our findings and recommendations and stated that it will reassess its ombudsman's role and reporting relationship.
Highlights: http://www.gao.gov/highlights/d06190high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−190

[Return to top]

Agriculture Sector

18. *December 15, Marshall Democrat−News (MO)* — **Officials play roles in agroterrorism exercise.** "What if?" That was the question Thursday, December 8, during an agroterrorism awareness and planning meeting held in Marshall as part of a series of meetings around the state sponsored by the Missouri Department of Agriculture. Southern District Commissioner Dick Hassler reported that about 22 persons. The daylong meeting focused on how county officials and others, including veterinarians and law enforcement agencies, would react in the event of an agroterrorism event or ag−related disease hitting the county. It also outlined which entities are responsible for which functions in the event of an emergency. Hassler said the second part of the meeting was dedicated to tabletop simulations. The group he was a part of was given the scenario of four lots of cattle purchased at a sales barn and headed to the county, with questions raised about how the cattle were put together into lots for sale and then a news report stating the animals may have been exposed to hoof−and−mouth disease.
Source: http://www.marshallnews.com/story/1131457.html

19. *December 15, Baltimore Sun (MD)* — **State takes more time on Asian oysters.** Maryland officials have extended their timetable for studying whether to introduce Asian oysters into the Chesapeake Bay. The Department of Natural Resources said Wednesday, December 14, that a committee overseeing the environmental impact study has decided to give researchers until at least June to complete their work. The committee, which includes Maryland Natural Resources Secretary C. Ronald Franks and his Virginia counterpart, W. Tayloe Murphy, will evaluate the status of the report then. The bay's native oyster population has been almost wiped out by disease and over harvesting. Where millions of oysters were once harvested, Maryland's take last season was 72,000 bushels, up from an all−time low of 26,000 bushels in 2004.
Source: http://www.baltimoresun.com/news/local/bal−md.oyster15dec15,1,5339542.story?coll=bal−local−headlines&ctrack=1&cset=true

[Return to top]

Food Sector

20. *December 15, Associated Press* — **E. coli outbreak traced to dairy that defied raw milk sales ban.** An outbreak of E. coli bacteria that has sickened 11 or more people, four critically, has been linked to a dairy that was ordered in August to stop selling raw milk. Dee Creek Farm, of Woodland, WA, accused of defying the order, is being investigated by at least four state and local agencies, and investigators asked that all of those who consumed milk from the dairy contact their local health departments, regardless of whether they are or have recently been ill. Cowlitz County prosecutors said Wednesday, December 14, that misdemeanor charges could be filed if the owners don't provide a list of customers who purchased raw milk. Eight E. coli sickness cases were confirmed in Clark and Cowlitz counties, all in children aged five to 14, and three apparent but unconfirmed cases were reported in nearby Clatsop, Ore. Four of the Washington state children were listed in critical condition in area hospitals. The popularity of

raw milk has grown in some quarters amid concern over genetically modified food and the use of hormones in livestock. Most people can drink raw milk without problems, but lack of adequate sanitation can result in contamination with E. coli and other bacteria.
Source: http://seattletimes.nwsource.com/html/localnews/2002685611_w ebecoli15.html

21. *December 15, Bloomberg* — **U.S. beef is on its way to Japan.** U.S. beef is already being shipped to Japan, just three days after the Asian nation reopened its market following a two−year ban over fears of mad−cow disease, U.S. Agriculture Secretary Mike Johanns said. U.S. meatpackers once had a one billion dollar market in Japan and Johanns said his department would work to rebuild that market share. "Beef is on its way, and we'll have beef in Japan by this weekend," Johanns said in an interview in Hong Kong Thursday, December 15, where he is attending the meeting of the World Trade Organization. More than 60 countries banned U.S. beef after a single mad−cow case was found in Washington state in December 2003. U.S. beef exports plunged to 434 million pounds in 2004 from a record 2.5 billion pounds in 2003.
Source: http://www.bloomberg.com/apps/news?pid=10000080&sid=aIqyExhq qBVs&refer=asia

[Return to top]

Water Sector

22. *December 14, U.S. Environmental Protection Agency* — **Tools to help small drinking water utilities control arsenic.** The U.S. Environmental Protection Agency (EPA) has released a set of user−friendly multimedia products to help small drinking water utilities meet revised regulations to control arsenic. The tools will provide owners and operators with information to guide them in making treatment decisions. The anchor product of this suite of tools is the Arsenic Virtual Trade Show, a learning portal for arsenic−treatment technology. The website features a database of vendors, a treatment "decision tree," and tips for evaluating and selecting treatment providers. Other products being released include: a brochure, which includes a checklist of questions that owners and operators of small utilities should ask treatment providers; a CD−ROM featuring commentary from the nation's top experts; and a DVD collection, which highlights arsenic treatment technologies currently being pilot−tested through EPA's Arsenic Treatment Technology Demonstration Program. In 2001, EPA revised the regulation for arsenic in drinking water to lower the maximum allowable level from 50 parts per billion to 10 parts per billion. The new standard becomes effective on January 23, 2006. The Agency estimates that more than 90 percent of the systems affected by the revised rule are small, serving populations of 3,300 or fewer.
Arsenic Virtual Trade Show: http://www.arsenictradeshow.org
Source: http://yosemite.epa.gov/opa/admpress.nsf/27166bca9a9490ee852 570180055e350/4da6ded5f66df8a3852570d7006f49c3!OpenDocument

[Return to top]

Public Health Sector

23.

December 15, Reuters — **Romania sees bird flu spreading to Bulgaria.** Romania confirmed cases of deadly avian flu in birds in five more villages in and around the Danube delta on Thursday, December 15, and warned migratory flocks could carry the virus south to neighboring Bulgaria. The highly pathogenic H5N1 virus has now been found in at least nine Romanian villages in the east of the country. The latest cases were confirmed after tests at a British laboratory. H5N1 is endemic in poultry in parts of Asia where it has killed 71 people since late 2003. "Flocks of migratory birds are heading to the northern parts of Bulgaria," Agriculture Minister Gheorghe Flutur told reporters, citing latest ornithologists' findings. "We sent a notification to the Bulgarian embassy." Bulgarian officials said precautionary measures against were being taken against the spread of the virus. Following outbreaks in Romania and its southern neighbor Turkey in October of the deadly H5N1 strain of the virus, Bulgaria has stepped up monitoring in poultry farms and wetlands for possible cases. Alexander Alexandrov, director of the state veterinarian office in northern Bulgaria, said birds had yet to land at their usual winter stopover at two lakes near the Black Sea.
Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=globalNews&storyID=2005−12−15T153844Z_01_DIT955645_RTRUKOC_0_US−BIRDFLU−ROMANIA.xml

24. *December 15, Associated Press* — **China reports sixth human case of bird flu.** China on Thursday, December 15, reported its sixth human case of bird flu. The latest human infection is a 35−year−old man in Suichuan County in the eastern province of Jiangxi. China has reported two confirmed human deaths from bird flu and a suspected case in a 12−year−old girl who died. Also Thursday, China reported a new bird flu outbreak on a poultry farm in the village of Shangxi, also in Jiangxi. It said 1,640 ducks were dead and 15,000 birds in the surrounding area were destroyed to stop the outbreak. The government statements didn't say whether the two cases in Jiangxi were believed to be linked. Authorities have reported 25 bird flu outbreaks in poultry around China since October 19. The government says 151,000 chickens, ducks and geese have died and another 22 million were destroyed to stop the outbreaks.
Source: http://abcnews.go.com/Health/wireStory?id=1408913

25. *December 15, San Francisco Chronicle (CA)* — **Whooping cough on rise throughout California.** Whooping cough, a disease that was largely tamed by vaccination, has been making a comeback throughout California, killing seven so far this year while the number of reported cases throughout the state has doubled. Also known as pertussis, whooping cough earned its nickname from the desperate noise that comes from the throats of infants and toddlers gasping for breath as they cough. Although children under one year of age are most vulnerable to pertussis, it strikes teenagers and adults as well. Nearly a quarter of the 2,169 California cases reported so far this year come from Fresno County, where more than 500 people from all age groups have come down with it. Last year, Fresno recorded only 15 cases. California's experience this year reflects a nationwide trend. There were 25,827 cases of pertussis reported in the U.S. in 2004 −− numbers that have been climbing slowly since 1976, when universal childhood vaccination programs brought the case count to an all−time low of 1,010. The steady rise −− punctuated by spikes in pertussis activity every three to four years −− has been puzzling to U.S. Centers for Disease Control and Prevention disease trackers since it was first noticed in the 1980s.
Whooping cough information: http://www.cdc.gov/doc.do/id/0900f3ec80228696/
Source: http://www.sfgate.com/cgi−bin/article.cgi?f=/c/a/2005/12/15/ BAGH2G860V1.DTL

26. *December 14, McGill University* — **Researchers crack genetic code of Quebec C. difficile.** Researchers at the McGill University, Génome Québec Innovation Center, and Jewish General Hospital have collaborated to successfully sequence the genome of a virulent strain of Clostridium difficile prevalent in Quebec, Canada, since 2003 and similar to strains elsewhere in the world. This marks the first time a strain of C. difficile has been sequenced in North America. The sequencing of this genome will allow researchers to develop improved detection, treatment, and prevention strategies for a strain of C. difficile responsible for more than three−quarters of cases in Quebec studied to date, as well as similar outbreaks in the U.S., and parts of Europe. The research team isolated the nucleic acid of the Quebec strain of C. difficile and made the breakthrough using ultra high−throughput sequencing technology at Washington University in St. Louis, MO.
C. difficile information: http://www.cdc.gov/ncidod/dhqp/id_Cdiff.html
Source: http://www.mcgill.ca/newswire/?ItemID=17823

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

27. *December 15, Los Alamos Monitor (NM)* — **New Mexico conference focuses on challenges in homeland security.** Experts in the fields of national security and counter−terrorism permeated New Mexico's fourth annual statewide homeland security conference at the Albuquerque Marriott Pyramid. Topics discussed by conference speakers included: emerging threats; cutting edge technological resources; expertise in conducting risk assessments; the formulation of appropriate response strategies; the development of inter−disciplinary partnerships to ensure the safety and security of federal, state and local communities; optimizing the Homeland Defense Equipment Reuse (HDER) program; cooperation and sharing of information and resources among regional entities; contagious disease warning signs, agriculture issues; border issues; risk based approaches to homeland security; master planning for homeland security; food supply protection; infrastructure protection; cyber security; detection of nuclear, chemical, biological and radiological weapons. Federal, state, local, and tribal personnel responsible for public safety attended the conference including those involved in law enforcement, emergency response, hospitals, corrections facilities and the military. "This conference is important because it's very difficult in a state like New Mexico to have meaningful training," said Ron Dolin, Los Alamos National Laboratory Center for Homeland Security Reachback coordinator. "New Mexico is a border state with level one targets of interest so the more we can help train our responders, the better prepared they will be."
Source: http://www.lamonitor.com/articles/2005/12/14/headline_news/n ews03.txt

28. *December 14, KLASTV (NV)* — **State Watch: Nevada homeland security program.** Las Vegas police use a program known as "City Watch" to help prevent terrorist attacks and

respond to disasters. The program connects the city to every security system on the Las Vegas Strip. It also includes government buildings and utilities. It runs on the Internet and can be accessed from anywhere so information will be available to first responders as well as incident planners. Following a demonstration of the Las Vegas City Watch program, members of the State of Nevada Homeland Security Commission voted to expand the program and made the recommendation to Nevada Governor Guinn to make it the State Watch program. Southern Nevada casinos, government buildings, and other companies already have already signed on. A link was established with their security systems and information was added for police and fire departments to access. In addition to maps, vital on−site equipment and where private security officers are stationed would be at the fingertips of emergency crews. The online program can be accessed from any computer or PDA, meaning first responders will have immediate access to in depth information about a situation. The program can even access security cameras at any building in the system.
Source: http://www.klastv.com/Global/story.asp?S=4246517&nav=168Y

[Return to top]

Information Technology and Telecommunications Sector

29. *December 14, Security Focus* — **Linux kernel find_target local denial of service vulnerability.** A local denial of service vulnerability affects the 'find_target' function of the Linux kernel. This issue is due to a failure of this function to properly handle unexpected conditions when attempting to handle a NULL return value from another function. This vulnerability may be exploited by local users to trigger a kernel crash, denying service to legitimate users. Solution: The vendor has released version 2.4.29 to address this issue.
For more solution detail: http://www.securityfocus.com/bid/14965/solution
Source: http://www.securityfocus.com/bid/14965/references

30. *December 14, Security Focus* — **Multiple unspecified Cisco catalyst switches LanD packet denial Of service vulnerability.** Multiple unspecified Cisco Catalyst switches are prone to a denial of service vulnerability. These devices are susceptible to a remote denial of service vulnerability when handling TCP 'LanD' packets. This issue allows remote attackers to crash affected devices, or to temporarily block further network routing functionality. This will deny further network services to legitimate users.
Source: http://www.securityfocus.com/bid/15864/references

31. *December 14, Tech Web* — **AT&T Security Chief says carriers should predict, prevent attacks.** A centralized military presence would be more effective in warning a neighborhood of incoming attacks than if each family sent grandpa up to their roof with field glasses. AT&T Chief Security Officer Ed Amoroso used that analogy to explain his company's strategy for fighting cyber attacks. "Every one of you is fighting the same cyber war," said Amoroso, a keynote speaker Wednesday, December 14, at Interop in New York City. Carriers have the power to detect problems by observing activity with a broad view. That, he said, puts them in a position to detect and prevent attacks of all kinds, rather than requiring each subscriber to individually erect firewalls and take redundant precautions against attacks. Though software creators need to improve their methods and reach for higher security standards, carriers must also take responsibility in providing much−needed improvements, he said. Amoroso said that

evolving applications need to be better integrated and better protected, especially with broadband leaving computers more vulnerable.
Source: http://www.techweb.com/article/showArticle.jhtml?articleId=1 75002779&pgno=1

32. *December 14, InfoWorld* — **Microsoft's security patches hit snag.** Some users of Microsoft Corp.'s Software Update Services (SUS) may be experiencing a minor annoyance, thanks to a glitch in the company's latest security patches, released Tuesday, December 13. The latest update may be changing the status of software updates that had been previously approved by administrators who use the service, according to Microsoft. "If you synchronize your server after December 12, 2005, all previously approved updates may be unapproved and the status may appear as 'updated,'" Microsoft said in a note published Wednesday, December 14. SUS is used by Microsoft administrators to gain more control over which Microsoft software patches get installed on their network. When a patch has been tested and determined to be appropriate for installation, it can be marked as "approved" and then automatically installed on the PCs being managed by the service. Tuesday's glitch disrupts that process. The problem is that the latest updates appear to have overwritten a file that is used to keep track of approved updates, said Russ Cooper, a scientist at security vendor Cybertrust Inc. The simplest solution is to simply restore this file, called Approveditems.txt, from a backup copy, Cooper said.
Source: http://www.infoworld.com/article/05/12/14/HNmspatches_1.html

33. *December 12, Tech Web* — **Security expert finds port scans not tied to hack attacks.** Port scanning, the practice of sniffing for computers with unprotected and open ports, isn't much of a harbinger of an attack, a University of Maryland researcher said Monday, December 12. Michel Cukier, an assistant professor at the College Park, MD,−based school, said that contrary to common thought, few port scans actually result in an attack. In fact, only about five percent of attacks are preceded by port scans alone. "But when you combine port scans with other kinds of scans, particularly vulnerability scans, there's a much higher probability of an attack," said Cukier. Nearly three−quarters of the attacks prefaced by some kind of scan came after both a port and a vulnerability scan were run against the exposed PCs, noted Cukier's report. Through his research, Cukier expected to see a higher correlation between port scanning and attacks, but the analysis also showed that it was relatively easy to spot the difference between a port scan and a more dangerous vulnerability scan simply by counting up the number of data packets received by the PC. Cukier and his researchers concluded that there seems to be no link between port scans and attacks.
Cukier's research paper: http://www.enre.umd.edu/faculty/cukier/81_cukier_m.pdf
Source: http://www.securitypipeline.com/news/175000553;jsessionid=M4 IGXZPVFH0JCQSNDBOCKHSCJUMEKJVN

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of a cross domain violation in Internet Explorer. This may allow a script in one domain to access web content in a different domain. Web browsers should adhere to the "Same Origin Policy", which prevents documents or scripts loaded from one origin from getting or setting properties of a document from a different origin. Internet Explorer does not follow this policy when importing CSS documents. For more information please see URL: http://www.mozilla.org/projects/security/components/same−ori gin.html

If the cross−domain violation in Internet Explorer occurs on a system that has Google Desktop Search (GDS) installed, then an attacker may be able to search for private data, execute programs, or execute arbitrary code on this vulnerable system. Google has modified its web pages to prevent exploitation of GDS through this particular vulnerability in Internet Explorer. The cross−domain violation vulnerability in Internet Explorer is still present, however. Although there is limited information concerning this vulnerability, US−CERT encourages users to disable Active scripting to prevent exploitation. For more information please review URL: http://www.cert.org/tech_tips/malicious_code_FAQ.html#ie566

Users can also refer to the Microsoft Security Response Center Blog for some additional information on this vulnerability affecting Internet Explorer. For more information please see: http://blogs.technet.com/msrc/archive/2005/12/07/415740.aspx x

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6346 (gnutella−svc), 80 (www), 6881 (bittorrent), 4142 (oidocsvc), 445 (microsoft−ds), 25 (smtp), 49889 (−−−), 135 (epmap), 53 (domain) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

34. *December 15, Government Accountability Office* — **GAO−06−322T: Hurricane Protection: Statutory and Regulatory Framework for Levee Maintenance and Emergency Response for the Lake Pontchartrain Project (Testimony).** The greatest natural threat posed to the New Orleans area is from hurricane−induced storm surges, waves, and rainfalls. To protect the area from this threat, the U.S. Army Corps of Engineers (Corps) was authorized by Congress in 1965 to design and construct a system of levees as part of the Lake Pontchartrain and Vicinity, Louisiana Hurricane Protection Project. Although federally authorized, the project was a joint federal, state, and local effort. For the levees in the project, the Corps was responsible for design and construction, with the federal government paying 70 percent of the costs and state and local interests paying 30 percent. As requested, the Government Accountability Office (GAO) is providing information on the (1) level of protection authorized by Congress for the

Lake Pontchartrain project; (2) authorities, roles, and responsibilities of the Corps and local sponsors with respect to the operation, maintenance, repair, replacement, and rehabilitation of the levees; (3) procedures in place to ensure that responsible parties maintain the levees in accordance with the authorized protection level; (4) authorities, roles, and responsibilities of the Corps and local parties when levees fail or are damaged; and (5) plans, capabilities, and activities that have been developed by the Corps to ensure an adequate emergency response when levees fail. GAO is not making any recommendations at this time.
Highlights: http://www.gao.gov/highlights/d06322thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−322T

[Return to top]

General Sector

Nothing to report.

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.